



Securing Critical Information Infrastructures

Training Course – Custom Parsing

Length – 16 Hours

Course Description

This course will train the students in the techniques and procedures needed to create custom parsing rules for the CS-MARS. This will allow the user to add new network devices to the existing device database and include them in incidents and reports. The information gathering and device testing will be covered in depth. Actual customer devices and/or logs can be used for the class project. The goal of this class is enable the students to be able to correctly add a new device to the network in an efficient and correct manner.

Course Outline

- What is custom parsing?
 - Gathering the necessary information to add a device
 - Pre-planning to understand what events are needed
 - Configuring the new device to work with CS-MARS
 - Using the CS-MARS tools to create a new device
 - Procedures and short cuts for adding the device
 - Testing the new device within CS-MARS
 - Integrating the device in the event logs and rules database
-

For more information on this or any other Lofty Perch training, contact us at training@loftyperch.com